What is claimed is:

1. A file security management method, comprising:

5   encrypting a file by using, as a key, position information which specifies a position in which the file can be opened;

saving the encrypted file;

decrypting the file by using, as a key, position

10   information which is detected by a position detecting device; and

displaying the decrypted file.

2. The file security management method

15   according to claim 1, wherein

a selection is made from among a plurality of preregistered positions when position information in which the file can be decrypted is selected.

20   3. The file security management method according to claim 1, wherein

a limitation is imposed on a position range in which the file can be opened by changing a data length of position information which is used as an encryption

25   key.

4. A file security management method, comprising:

saving data that is encrypted by using, as a key, position information which specifies a position in which the data can be used, and the position information as a key;

determining whether or not position information which is detected by a position detecting device and the saved key match, and decrypting the encrypted data by using the key if the position information and the saved key match; and

displaying the decrypted data.

5. A file security management apparatus, comprising:

an encrypting unit encrypting a file by using, as a key, position information which specifies a position in which the file can be opened;

a saving unit saving the encrypted file;

a decrypting unit decrypting the file by using, as a key, position information which is detected by a position detecting device; and

a displaying unit displaying the file decrypted by said decrypting unit.

6.   A   file   security   management   method,
comprising:

encrypting a file by using, as a key, position
5   information which specifies a position in which the file
can be opened; and

saving the encrypted file.

7.   A   file   security   management   method,
10   comprising:

decrypting an encrypted file by using, as a key,
position information which is detected by a position
detecting device, when opening the file; and

displaying the decrypted file.

15

8.   A   file   security   management   method,
comprising:

encrypting data by using position information
which specifies a position in which the data can be used;
20   and

transmitting the encrypted data, or saving the
encrypted data onto a computer-readable storage medium.

9.   The   file   security   management   method
25   according to claim 8, wherein

a limitation is imposed on a position range in which a file can be opened by changing a data length of position information used as an encryption key.

5   10.   A computer-readable storage medium on which map information is recorded, wherein:

map data encrypted with position information which specifies a position in which a user can use the map data is recorded; and

10   map data, which can be decrypted only if position information detected by a position detecting device and the position information used to encrypt the map data match, is recorded.

15   11.   A program security management method, comprising:

encrypting a program with position information which specifies a position in which the program can be used; and

20   transmitting the program encrypted with the position information, or saving the encrypted program onto a computer-readable storage medium.

12.   The program security management method

25 according to claim 11, wherein

the program is encrypted with the position information, and a license key given to a user.

13. A computer-readable storage medium on which is recorded a program that is encrypted with position information which specifies a position in which the program can be used.

14. A program security management method, comprising:

encrypting a program with position information which specifies a position in which the program can be used;

transmitting the program encrypted with the position information, and a license key given to a user;

receiving, by the user, the encrypted program and the license key; and

decrypting the encrypted program with position information which is detected by a position detecting device, and the license key.

15. A file security management apparatus, comprising:

encrypting unit encrypting a file by using, as a key, position information which specifies a position

in which the file can be opened; and

saving unit saving the encrypted file.

16. A file security management apparatus,
5   comprising:

a decrypting unit decrypting a file by using, as
a key, position information which is detected by a
position detecting device; and

a displaying unit displaying the file decrypted
10   by said decrypting unit.

17. A computer-readable storage medium on which
is recorded a security management program for causing
a computer to execute a process, the process comprising:
15   encrypting a file by using, as a key, position
information which specifies a position in which the file
can be opened;

saving the encrypted file;

decrypting the file by using, as a key, position
20   information which is detected by a position detecting
device, when opening the file; and

displaying the decrypted file.

18. The computer-readable storage medium
25   according to claim 17, the process further comprising

imposing a limitation on a position range in which the file can be opened by changing a data length of position information used as an encryption key.

5   19.   A computer-readable storage medium on which is recorded a security management program for causing a computer to execute a process, the process comprising:

encrypting a file by using, as a key, position information which specifies a position in which the file

10   can be opened; and

saving the encrypted file.

20.   A computer-readable storage medium on which is recorded a program for reading map data from a storage

15   medium on which is recorded map data encrypted with position information which specifies a position in which the map data can be used, the program comprising

allowing the map data to be decrypted only if position information detected by a position detecting

20   device and the position information used to encrypt the map data match.